"Home Security System: Motion-Sensing Cameras, Lights, Automated Door, and Alerting Device for Burglary Prevention"

Research Proposal for
Research IV

Members:
Cañabano, Greg Nathaniel M.
Diamano, Rick Steven
Monding, Isidore Klein I.
Salboro, Marrence M.
Urciada, Christian Xianirant S.

Teacher:
Mrs. Dallie G. Elum

Date of Submission:
September 13, 2024

INTRODUCTION

Crime in the Philippines is one of the major problems the country has to deal with today, with some major crimes being theft of property, robbery, and burglary. With a report from the Philippine National Police stating 13,469 crime incidents happened between the period of January until May 13, 2023**.** But it has to be mentioned that the crime incidents of that time decreased by 10% compared to the previous year which had a total of 15, 064 crime incidents that happened in the same period (Argosino, 2023)**.** Though it has decreased, the crime rate is still high and should be lowered as much as possible with proper law enforcement and primarily by the citizens themself by using alternative ways to prevent such crimes from happening.

One of the common crimes being committed in the modern era is burglary, burglary is defined as the act of breaking and entering a building like a house or a commercial building in order to commit a felony like theft (Merriam-Webster, 2024). Burglaries often happen due to the lack of security in a household, leaving windows and doors open, or having features in the house that are susceptible to exploitation to individuals wanting to get in (Metropolitan Police, 2024). Homes that leave expensive packages or vehicles outside their house are also at a higher risk of being targeted by individuals looking for property to steal (Metropolitan Police, 2024). These types of crime are more likely to happen in residential areas according to a statistical report conducted in 2022, where homes are reported to have 386,489 burglary incidents in the United States alone, that is 58% of all burglary incidents (Korhonen, 2024). Only a small number of these cases are properly solved, with a percentage of 12.1% (Gramlich, 2024). Another report by the Federal Bureau of Investigation (2023) reported that 184,846 cases of burglaries at a residence occur at night and a further 239,137 cases occurring at day time. It is clear that the rate of burglaries in the United States alone shows how this type of crime is a common problem by ordinary citizens or civilians.

The researchers aim to combat this type of crime by creating a system that will monitor the perimeter of a household and potentially alert the homeowner if there are any attempts of burglaries into their private residence. The researchers also considered that this should be a user-friendly system to all disabled individuals and normal people by developing a wireless opening door system that will have 2 factor authentication for added security. The researchers will consider the safety of the door opening system and time it will take for an alarm to reach the homeowner. The system will have motion sensors connected to cameras, lights, and speakers that will be designed to record and state that the criminal is being filmed, both working in the day or in the night. The researchers will also create a history log where it will show the different times the system detects movement using the motion sensors, or when the door is used and opened by a person.

The study is significant as the researchers hope to counteract burglary by the use of this security system as a way of having ease of access, home security, crime prevention, to alert of a crime, and possibly aid in solving such crime cases. Having an automatic door automatically open every time you want to enter the household will be much easier of a task especially if an individual is carrying items or if they are a disabled. Having the cameras and lights will also help in home security as a way for an individual to feel safe in the comfort of their own home. Burglaries are less likely to happen if an individual sees that the residence contains cameras or a security system, they are also likely to target a home repeatedly if they see the homeowner failed to put and upgrade their security system (Metropolitan Police, 2024). Having a security system being visible will serve as a deterrence against any intruder that may attempt to break-in a person's home. The system can also help in case the homeowner is not at their residence, it will be able to alert them if any suspicious activities and movement is detected in the perimeter of the house. This will give the owner enough time to call the police if ever there is a burglary being committed on their property. And lastly, the system would also be helpful in any crime case, not just burglaries, as it can aid investigators to solve criminal cases through the use of the history log that the system will have. Where it contains videos of activities or motion being detected and recorded by the cameras along with dates and time being provided, this could serve as useful pieces of information that they could possibly use.

The primary research question addressed in this study is as follows:

Main Problem: How reliable is the HSS-MCLADA Device (Home Security System: Motion-Sensing Cameras, Lights, Automated Door, and Alerting Device for Burglary Prevention) in detecting, preventing, and alerting users about unauthorized access?

This main problem is broken down into the following sub-problems:

Sub-Problems:

1. How reliable are the motion-sensing lights and cameras in consistently detecting and responding to unauthorized movements?
2. How reliable are the automated doors in providing secure and seamless access control while preventing unauthorized entry?
3. How reliable is the alarm system in promptly alerting users to potential security breaches?

4. How safe is the automated door in the process of opening and closing, especially regarding user safety and preventing accidental injuries?

In conducting this study, the researchers will be testing the following hypotheses:

Null Hypothesis (Ho): The system's components—motion-sensing lights and cameras, automated doors, and alarm systems—will not work as expected in preventing or detecting unauthorized entry (a, b, or c will not work).

Alternative Hypothesis (Ha): The system's components—motion-sensing lights and cameras, automated doors, and alarm systems—will effectively work together to prevent and detect unauthorized entry, as well as alert the homeowner to potential threats (a, b, and c will work).

The scope of this study focuses on the implementation of the HSS-MCLADA Device (Home Security System: Motion-Sensing Cameras, Lights, Automated Door, and Alerting Device for Burglary Prevention) within residential areas. Specifically, the system is designed to cover the perimeter surrounding the household, concentrating on entry points like doors and windows, which are the most vulnerable areas for burglaries. The system will operate with real-time, 24/7 monitoring, ensuring continuous surveillance both during the day and at night. The integration of motion-sensing lights and cameras, automated doors, and an alerting system guarantees round-the-clock protection, enhancing the security of the residence. Additionally, the system is intended for homes located in areas with cellular signal or reliable internet connectivity. This is critical for enabling remote alerts, allowing homeowners to receive real-time notifications about any suspicious activities, no matter where they are. The system's functionality depends on this communication network, making it suitable for both urban and suburban homes that have access to these services.

The delimitations of the study include a focus on residential buildings only. Commercial or industrial buildings, which have different security needs, are beyond the scope of this research. Furthermore, the system is designed to contact only the homeowner during potential security breaches, rather than alerting local authorities or emergency services directly. This decision emphasizes personal control over security and leaves the responsibility of contacting law enforcement to the homeowner. Moreover, the study is limited to the security aspects of home automation, specifically addressing burglary prevention. It will not explore broader smart home features such as climate control or energy management. The HSS-MCLADA Device is engineered to prevent burglary, and it alerts the homeowner if unauthorized entry or suspicious movements are detected. Other threats, such as fire, flooding, or natural disasters, are not within the scope of this system. By focusing solely on security and burglary prevention, the research aims to provide an efficient and practical solution to reduce crime in residential areas.

REVIEW OF RELATED LITERATURE

A study conducted by Amole et al.(2019) developed an infrared sensor controlled automatic sliding door that proved to be successful in overriding the manual operation of a sliding door. The results showed that the door was characterized by average opening time, closing time, delay time, and optimal sensing range of 3.10 s, 3.05 s, 5.72 s, and 23.5 cm, respectively, they concluded from these results that the study was successful. The researchers of the HSS-MCLADA device will incorporate a similar infrared sensing system in the automation of the door and the motion-sensing ability of the cameras & lights. Infrared and Bluetooth will be combined to create a two-factor authentication wherein the door will check for the presence of a human in front of it and check if there is a valid Bluetooth signal being received, once both factors are verified, the door will open. This helps make the door more secure as not only does it check for movement or presence of humans but also identifies if the human/s present are the homeowners to open the door.

While the study conducted by Hoque (2022) focuses on the overall IoT-enabled security system, it incorporates motion sensors, including Passive Infrared (PIR) sensors, as part of the security architecture. These sensors are vital for detecting movement in the environment, especially at entry points like doors. Once movement is detected, the system can trigger web cameras for real-time surveillance, capturing footage of any unauthorized activity. The use of motion sensors in conjunction with cameras was proven effective for real-time surveillance. The motion detection would trigger the camera only when necessary, minimizing unnecessary recording and saving power. However, the study also noted that external factors, like radio frequency interference, could impact the reliability of sensors, requiring careful consideration in deployment. In our HSS-MCLADA system, the motion-sensing cameras serve a central role in ensuring the security of residential spaces. Just as in the previous study, we will be using PIR motion sensors to activate cameras only when motion is detected, thereby optimizing camera usage and improving energy efficiency. This approach not only helps in reducing false alarms but also enhances the reliability of the system by focusing on real-time threats. Moreover, by utilising the cost-effective nature of motion-sensing cameras, our research aligns with the emphasis on efficient, real-time surveillance systems, further supporting the practicality and effectiveness of our home security solution.

Another study conducted by Villanueva et al.(2023) created a device with a purpose to alarm the owner of an item if it was stolen, using Arduino Uno's PIR motion sensor and tilt ball switch sensor; the device can be installed in the doors, cabinets, or lockers of a residential building or any other buildings. The PIR motion sensor detects any intruder or unwelcome guest within the vicinity of the device with a certain range, while the tilt ball switch sensor detects if the door, cabinet, or locker is forcibly opened in some way. They used a GSM module and a sim card in order to establish communication and alarm the owner of the item if ever stolen. The study concluded that the alerting system using a GSM module and a sim card executed their function efficiently while the PIR motion sensor was inefficient in detecting high speed objects, with the researchers stating that it is better to use other motion sensing technologies. It is important to highlight that the GSM module and the sim card can possibly be used in other studies relating to directly giving an alarm to an individual's phone, in a way detecting theft or burglary like the HSS-MCLADA.

According to research by L. Bangali and P. Shaligram (2013), Arduino systems are highly adaptable for embedded applications like security systems. The systems can handle multiple tasks simultaneously using interrupts, which efficiently manage RFID or Bluetooth signal detection. This frees up processing power for critical tasks such as controlling actuators and sensors. The multitasking capability of Arduino is crucial for the MCLADA system, as it allows simultaneous response to Bluetooth signals, door control, and security monitoring. Real-Time Engineers Ltd (2023) explains that FreeRTOS enhances Arduino's multitasking abilities by enabling true concurrency, scheduling different processes independently. For the MCLADA system, FreeRTOS would ensure simultaneous monitoring of security threats and real-time access to authorized users without performance lag. Additionally, according to C. Coleman (2020), time slicing, or cooperative multitasking, allows Arduino to efficiently manage different tasks, making it crucial for maintaining a responsive and secure environment, especially for individuals with difficulty managing traditional locks.

In a study by S. Anand et al. (2019), Bluetooth technology is presented as a dependable alternative to RFID for access control systems. This enables seamless interaction between a user’s smartphone and the Arduino system, allowing hands-free access to doors. The use of Bluetooth simplifies the process, particularly benefiting individuals with physical disabilities, as it eliminates the need for physical interaction with a tag or card. M. Lubbers et al. (2019) also highlight that Arduino’s use of C/C++ programming language is well-suited for applications requiring real-time control of hardware components, such as door automation systems. This language provides direct access to Arduino’s hardware features, ensuring efficient management of Bluetooth modules and motor controls. Consequently, C/C++ is an appropriate choice for the MCLADA system, enhancing both its responsiveness and reliability while maintaining security.

METHODOLOGY

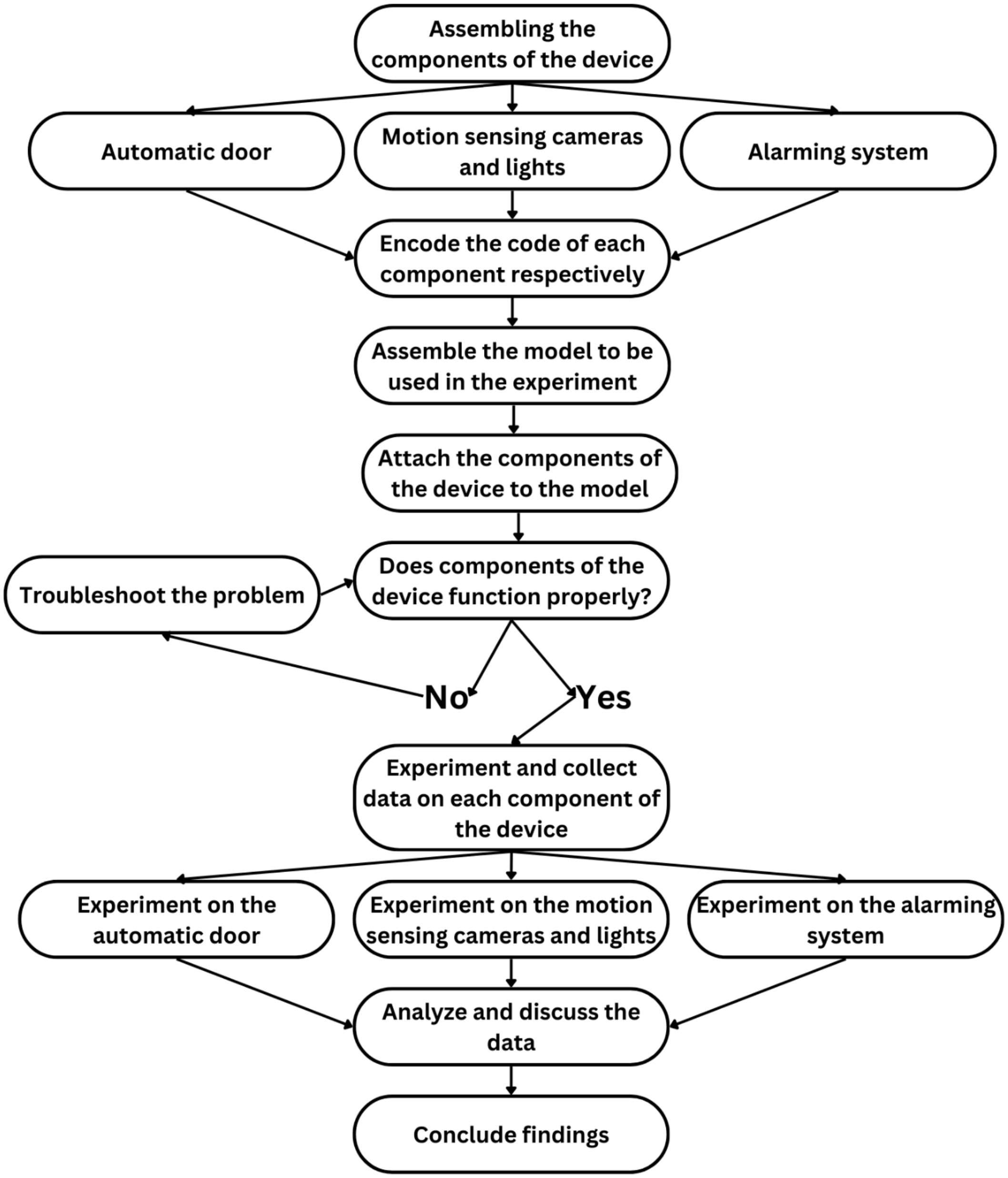
Research Design

The research design for study will be experimental. This approach will allow the researchers to figure out the effectiveness of HSS-MCLADA along with all its components which are the motion sensing lights and cameras, automatic opening door, and the alerting system, in properly executing their functions.

Table 1: Materials

HC-05 Bluetooth Module	GSM Module	Arduino UNO	24V Stepper Motor	24V and 5V DC Source	Reed Switch Window/Door Sensor	USB Cable
Multimeter	Screws	Nails	Hammer	Plywood	Breadboard	Screw driver
Hammer	Soldering iron	Male and Female Jumper Wires		Laptop	Drill	Soldering lead
Soldering paste	Resistor	OV7670 Camera Module	HC-SR501 PIR Sensor	Gear	Sound Output Module	

Figure 1: Conceptual Framework



Procedures

1. Construction of the Model

The first step in the research is constructing a working prototype of the HSS-MCLADA system. This model will simulate a typical household setup, including doors, windows, and entry points, to test the effectiveness of the security system components.

1.1 Materials Required:

- Plywood (to build a mock door and window setup)
- Screws, nails, hammer, drill (for construction)
- Stepper motor and gear mechanism (for door automation)
- Breadboards, jumper wires, resistors (for wiring components)
- OV7670 Camera Module
- HC-SR501 PIR motion sensors
- HC-05 Bluetooth module
- GSM module
- Arduino UNO microcontrollers
- 24V and 5V DC power sources
- USB cable
- Multimeter
- Laptop (for programming and testing)

1.2 Steps for Construction:

1. Mock Door and Window Setup: Using plywood, construct a simulated door and window setup, similar to residential entry points.

2. Mount Cameras and Sensors: Install the OV7670 camera, PIR motion sensors, and lights on the mock door and window frames. These components will monitor movement at entry points.

3. Automated Door Mechanism: Attach a stepper motor and gear mechanism to the door. This motor will automate the opening and closing process in response to Bluetooth signals.

4. Power Supply Installation: Set up a 24V and 5V DC power supply to ensure the cameras, sensors, and motors are powered continuously. Wire the components to the power source using breadboards and jumper wires.

5. Alert System Setup: Install the GSM module, which will be used to send alerts to the homeowner in case of unauthorized access.

6. Bluetooth Module Placement: Install the HC-05 Bluetooth module, which will pair with the homeowner's smartphone to control the automated door.

7. Connect all the components through the use of a breadboard to the Arduino UNO microcontroller.

2. Installation of the System

Once the model is constructed, the next step is to install the HSS-MCLADA system in a controlled environment where experiments will be conducted. This will simulate real-world conditions to test how well the system performs.

2.1 Installation Steps:

1. Component Integration: Connect all system components—motion sensors, cameras, automated door mechanism, Bluetooth module, and GSM alerting system—using Arduino microcontrollers. Ensure each component is wired correctly and functions as intended.

2. Power Source Connection: Verify that each component receives the appropriate voltage for operation.

3. Bluetooth Setup: Pair the HC-05 Bluetooth module with a smartphone. This device will trigger the automated door to open and close upon detecting an authorized Bluetooth signal.

4. System Placement: Install the cameras, sensors, and door mechanism at strategic locations within the experimental setup to monitor entry points.

5. Initial Testing: Conduct a preliminary test to ensure that all components (cameras, sensors, door mechanism, and GSM module) are functioning correctly before starting the full experiment.

Figure 2: Door Exterior (Front)

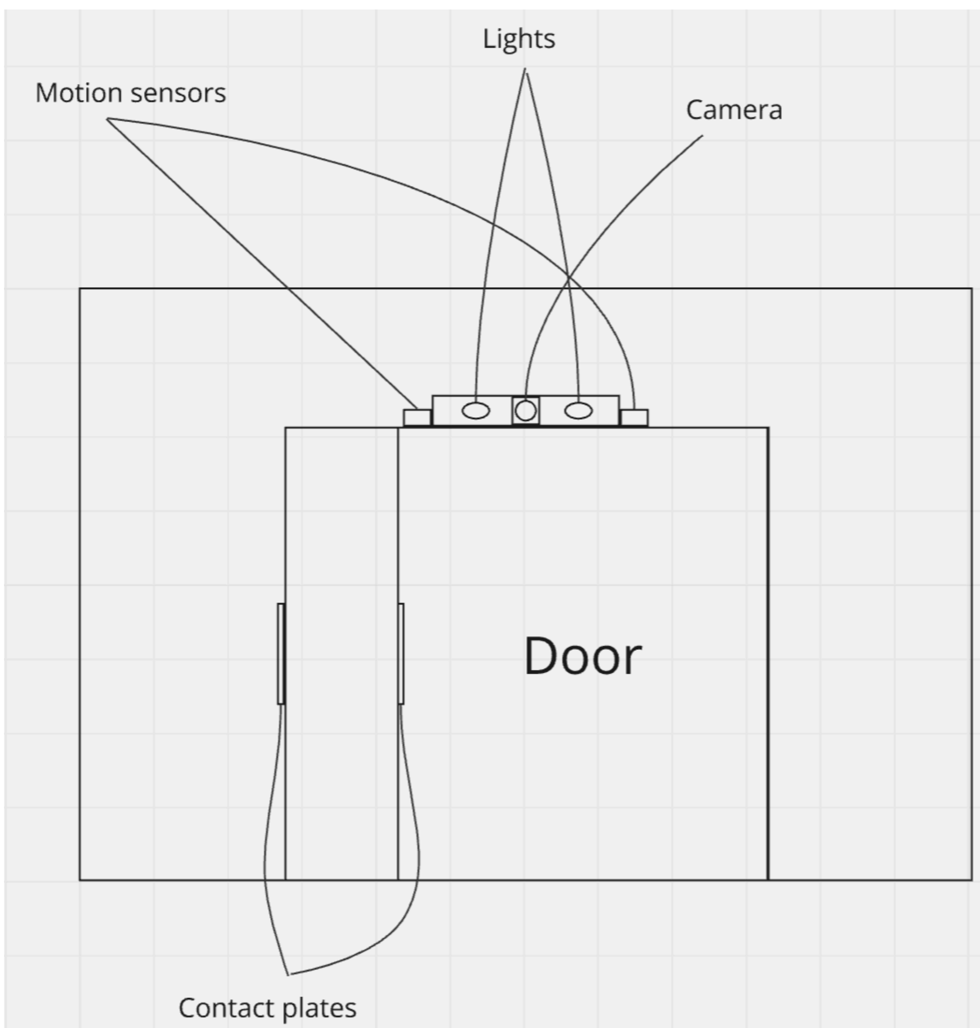


Figure 3: Door Interior

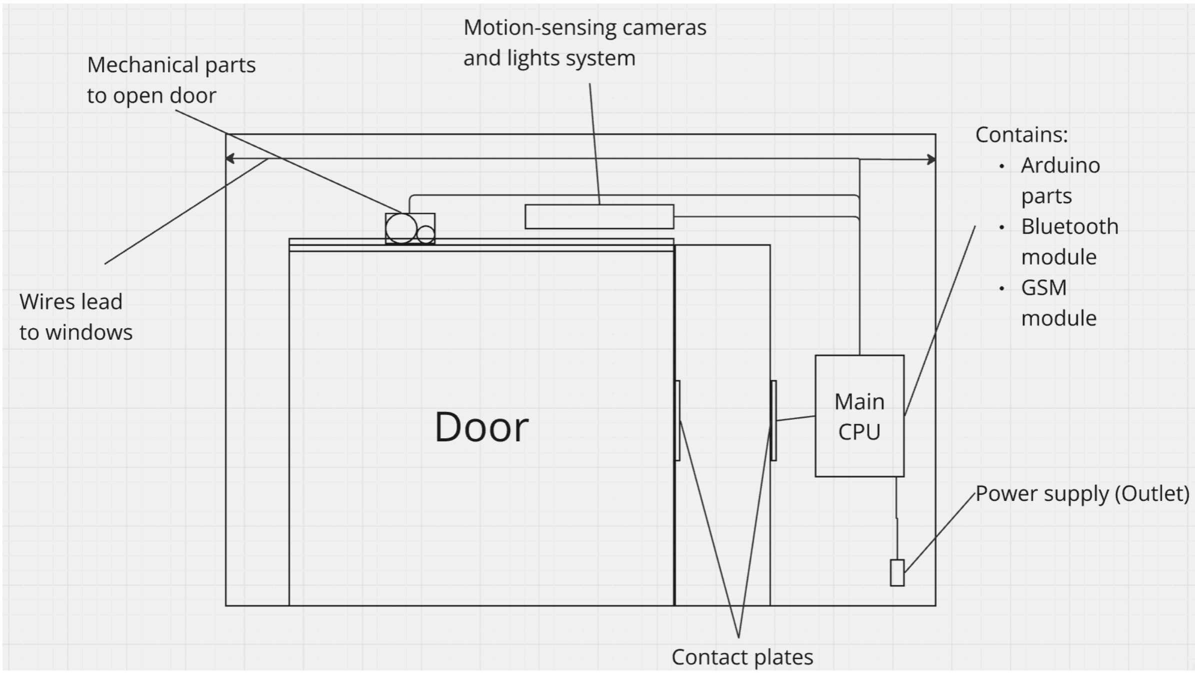


Figure 4: Window Exterior (Left and Right)

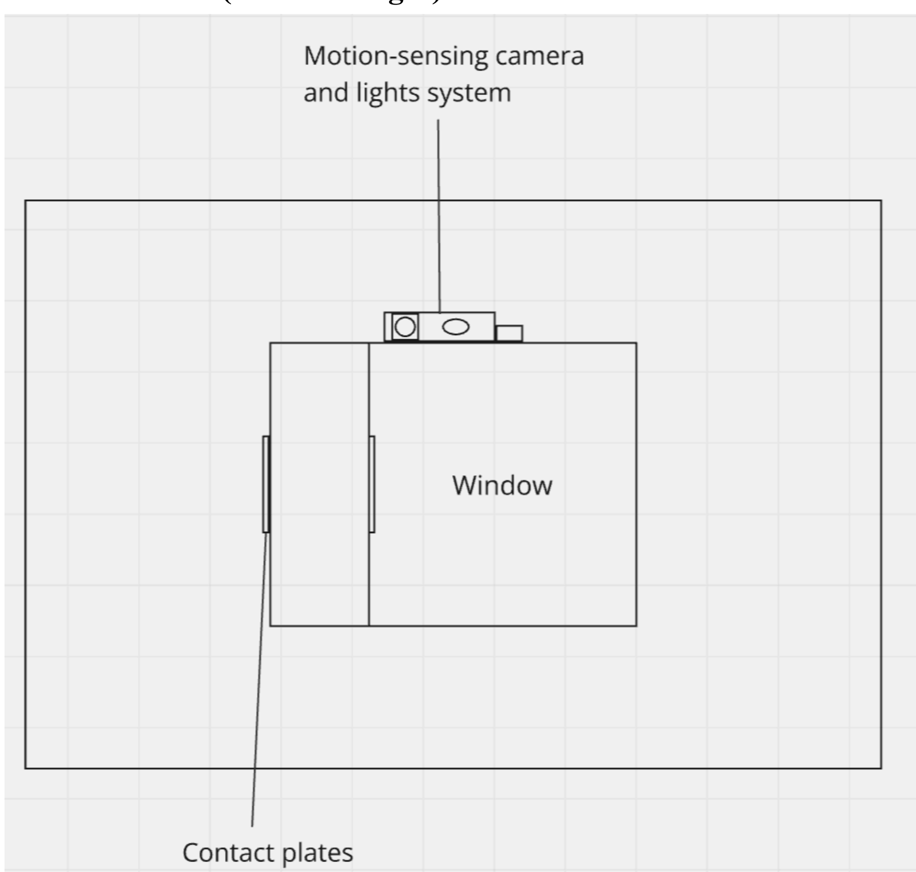


Figure 5: Window Interior

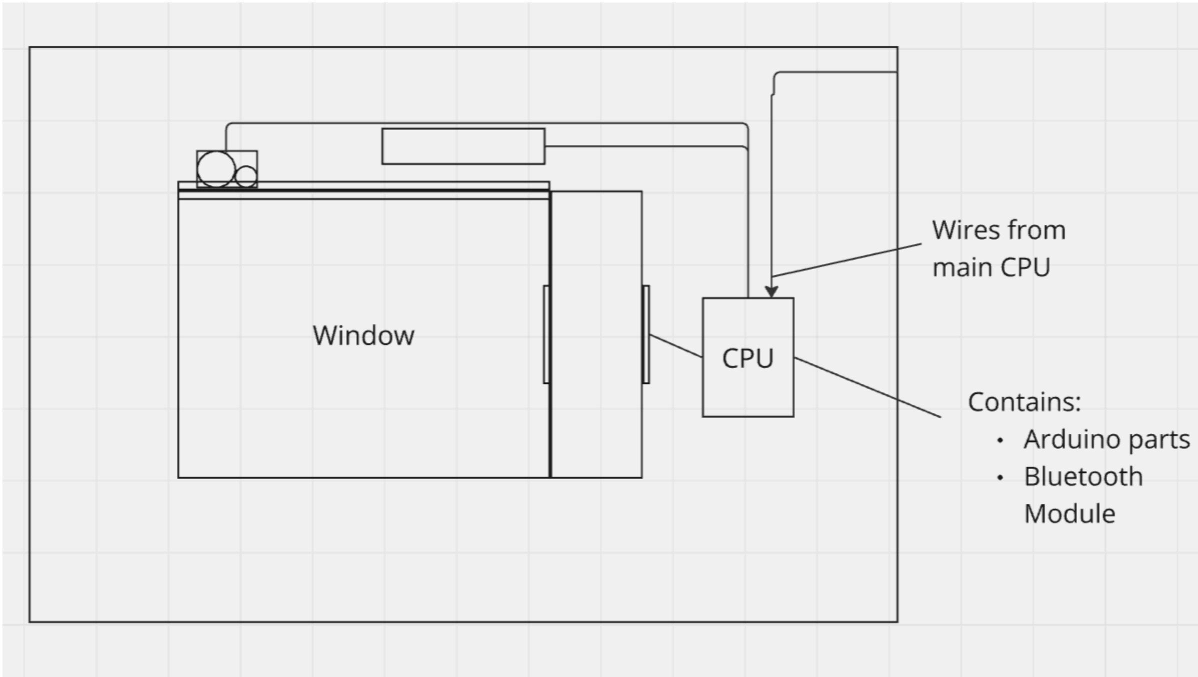
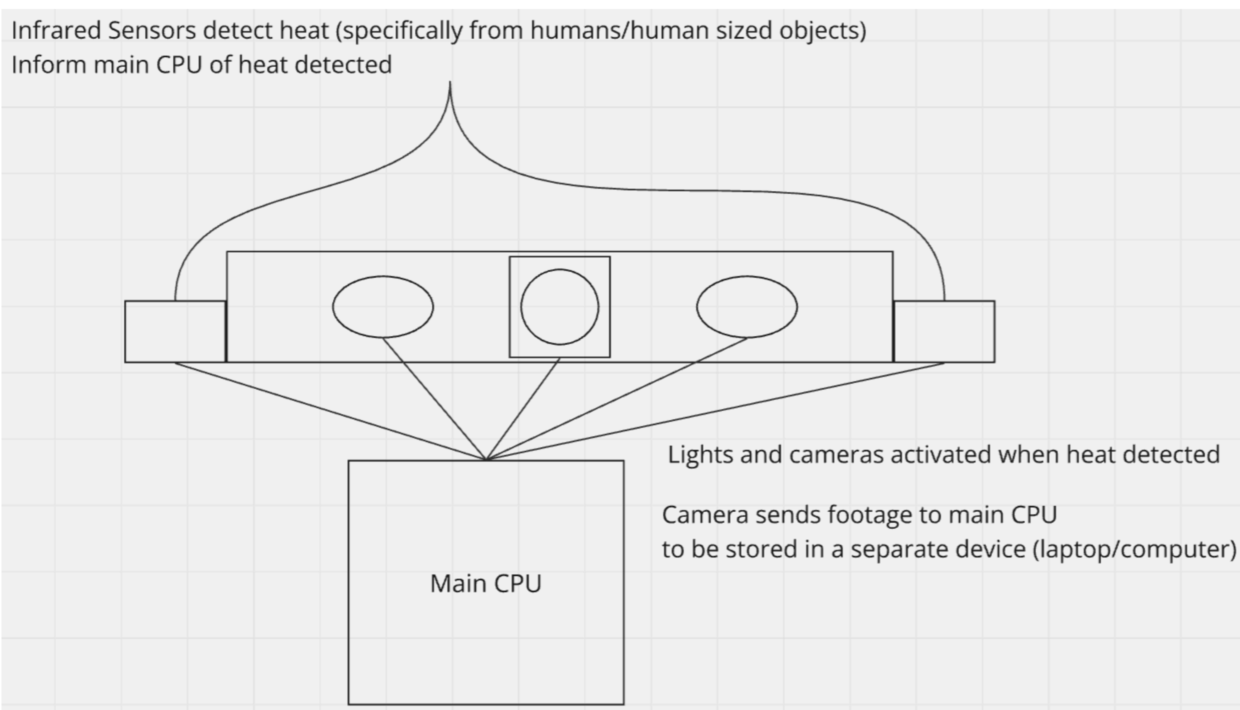


Figure 6: Motion-sensing cameras and lights



Data Collection

The data will be collected from 4 different sets of experiments that will test the reliability of the 3 components of HSS-MCLADA, alongside with the testing of automatic door safety of use by users as well. The motion sensing lights and cameras will be tested in a way where we can determine the reliability of the motion sensors in detecting movement. The automatic door will be tested by how reliable or if it executes its function properly given a set amount of trials. The alerting system will be tested by how fast it can reach or notify the homeowner given a set amount of trials. And lastly, the safety of the automatic doors will be tested by testing if it would close if an object or person is still between the doors.

The experiments will focus on evaluating the reliability of each system component, as well as the integrated functionality of the HSS-MCLADA system. The following experiments will be conducted:

1. Motion-Sensing Lights and Cameras Testing

This experiment will assess how accurately the motion sensors detect movement and activate the cameras and lights in response.

- Steps:

1. Simulate movement near the PIR motion sensors to trigger the system. The cameras and lights will activate upon detecting motion.
2. Record the time between motion detection and activation of the cameras and lights.

3. Repeat the test 50 times for each treatment (Small sized object, medium sized object, large sized object), and log the results to determine detection accuracy and response times.

4. Calculate the number of true positives (accurate detections) and false positives (erroneous triggers) for each treatment.

2. Automated Door Reliability Testing

The automated door will be tested for its ability to open and close reliably when it detects an authorized Bluetooth signal.

- Steps:

1. Use a Bluetooth-enabled smartphone to trigger the door's opening mechanism. The stepper motor will control the door based on the Bluetooth signal.

2. Conduct the test at varying distances (e.g., 1 meter, 2 meters, 3 meters) to assess how quickly the door responds.

3. Record the time it takes for the door to open and close, and log successful and unsuccessful attempts.

4. Repeat the test 50 times, ensuring both valid and invalid Bluetooth signals are used.

3. Alerting Device Response Time Testing

This experiment will evaluate the GSM module's ability to send alerts to the homeowner in case of unauthorized access.

- Steps:

1. Simulate unauthorized access to the system by triggering the motion sensors without using a paired Bluetooth device.
2. Monitor the GSM module's response time in sending an SMS alert to the homeowner.
3. Conduct trials at various distances from the GSM network, simulating different signal strengths.
4. Record the time taken for the alert to reach the homeowner and repeat the test 30 times for each treatment or distance to determine average response times.

4. Automated Door Safety Testing

This experiment will assess the safety features of the automated door, specifically its ability to detect obstructions and prevent accidents.

- Steps:

1. Test the door's ability to stop closing when an object (such as a hand or block) is placed in its path.
2. Run 50 trials, with objects placed at different points during the door's closing process (early, middle, and near complete closure).
3. Record whether the door stops safely upon detecting an obstruction and measure response times.

DATA ANALYSIS & FINDING

Descriptive statistics include percentages, means, and response durations, all of which summarize the effectiveness of the system's components. These types of measures provide a total picture of the system regarding operational effectiveness in different scenarios. Descriptive statistics enable the summarizing of large amounts of data so that clarity of system performance becomes clearer. For example, determining the average time to respond shows how dependable the system is in its response to threatening parameters. The percentages include the success rate of entries, whereas the ratio determines the dependability of the door. Each component's accuracy and false alarm rates are determined by the true positives, false positives, and false negatives. The metrics of precision and frequency of errors shall be based on cross-validation of every detection, alarm, and access event against a pre-validated ground truth, one that involves either video recordings or system log to determine if each system decision was correct. For example, if there is no individual but the system detects motion; that is a false positive. These rates provide quantification so one can know how well the system discriminates against a legitimate threat versus an incorrect alarm.

Reliability testing measures how consistently the system performs over time. This usually involves monitoring the failure rates and ensuring whether or not the system behaves accordingly under natural conditions. Reliability testing keeps the system running, operating consistently and effectively over time. Such an example involves analyzing the rates of failure, which tells whether things such as automated doors and cameras degrade in performance or malfunction quite often. This is done through periodic monitoring of the system over a predetermined period and the calculation of how often errors come up.

The HSS-MCLADA device will be able to detect unauthorized access correctly with few numbers of false alarms. The automated door is foreseen to serve well and yield a minimum number of successful access to unauthorized persons. The alerting mechanism should provide timely notification to the home owners for fast awareness of security breaches.

The contribution of this study will add practical connotations to the development of home security systems through highlighting the imperatives of such devices regarding speed, accuracy, and safety. Theoretically, the paper contributes to the existing literature on integrated security systems by providing empirical data about the efficiency of motion detection, automated doors, and alerting mechanisms for security at residential levels. This can be a starting point for further technologically enhanced home security solutions.

In future studies, the scalability of the system for larger houses or commercial buildings can be investigated to find out if the performance of the device holds constant in a more complex environment. AI-based analytics also can be integrated with the system for higher accuracy in detecting false positives and further reduce response times. Research may be conducted that concentrates on the improvement of user experience, in particular for elderly or disabled persons who need more accessible security systems.

REFERENCE LIST

Amole et al. 2020. Design and implementation of a prototype active infrared sensor controlled automatic sliding door for mitigation of coronavirus disease 2019 (COVID-19). https://repository.acu.edu.ng/handle/123456789/359

Arduino. (2020). Using interrupts with Arduino. https://www.arduino.cc/reference/en/language/functions/interrupts/interrupts/

Bhatia, S., & Gupta, A. (2020). RFID-based automatic door locking system: A security enhancement. International Journal of Computer Applications, 975, 1-5. https://www.ijcaonline.org/archives/volume975/number1/10833-2019

Bluetooth. (2019). Key attributes of Bluetooth: Range. https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/

Catania, A., & Mazzola, A. (2019). Cooperative multitasking on Arduino: A practical approach. Journal of Embedded Systems, 2019, 1-10. https://doi.org/10.1155/2019/1234567

Circuit Basics. (2020, June 30). How to optimize your Arduino code. https://www.circuitbasics.com/how-to-optimize-arduino-code/

Elektor Magazine. (2020, April 30). Arduino compiler optimizations for faster & smaller code. https://www.elektormagazine.com/labs/arduino-compiler-optimizations-for-faster-smaller-code

Federal Bureau of Investigation. (2023). Property crime statistics. https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/explorer/crime/property-crime

Forbes. (2023, January 10). Home invasion statistics. https://www.forbes.com/home-improvement/home-security/home-invasion-statistics/

FreeRTOS. (2020). FreeRTOS on Arduino. https://www.arduino.cc/reference/en/libraries/freertos/

FreeRTOS. (2017). RTOS - Free professionally developed and robust real time operating system for small embedded systems development. https://www.freertos.org/RTOS.html

Gunawan, A., Kurniawan, A., & Setiawan, A. (2021). Integration of FreeRTOS with Arduino for real-time control applications. 2021 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM), 1-6. https://ieeexplore.ieee.org/abstract/document/9609710/

Inquirer.net. (2023, June 15). PNP index crimes in PH down by 10% in January to May 2023. https://newsinfo.inquirer.net/1769308/pnp-index-crimes-in-ph-down-by-10-in-january-to-may-2023

Last Minute Engineers. (2022). HC-SR501 PIR sensor tutorial. https://lastminuteengineers.com/pir-sensor-arduino-tutorial/

McGowan, M., & McGowan, A. (2018). Using FreeRTOS with Arduino: A guide to multitasking. Electronics Projects for Beginners. https://www.electronicwings.com/nodemcu/using-freertos-with-arduino

Merriam-Webster. (2024). Burglary definition. https://www.merriam-webster.com/dictionary/burglary

Metropolitan Police. (2017). Residential burglary facts.

https://www.met.police.uk/cp/crime-prevention/protect-home-crime/residential-burglary-facts/

Hoque, M. (2019). Design and Implementation of an IoT-Based Smart Home Security System https://doi.org/10.37624/IJERT/11.5.2022.1-6

Pew Research Center. (2024, April 24). What the data says about crime in the U.S.

https://www.pewresearch.org/short-reads/2024/04/24/what-the-data-says-about-crime-in-the-us/

Statista. (2023). Burglary in the U.S. by location of felony.

https://www.statista.com/statistics/195200/burglary-in-the-us-by-location-of-felony/

Villanueva, M. J. S., Bacorro, D. M., Guilas, Y. F. H., Khoe, J. J. D., Madarcos, M. A., Pastrana, Z. K. G., Bautista, Z. K., & Limos-Galay, J. A. (2023). Theft alarm system using Arduino Uno's PIR motion and tilt ball switch sensors. *International Journal of Research Studies in Management*, 11(3), 11-20. https://doi.org/10.5861/ijrsm.2023.1023

BUDGET AND EXPECTED SCHEDULE

Table 2: Budget

Materials:	Prices:
Gear mechanism	₱60.00
Breadboards, jumper wires, resistors	₱500.00
OV7670 Camera Module	₱100.00
HC-SR501 PIR motion sensors	₱60.00
HC-05 Bluetooth module	₱150.00
GSM module	₱500.00
Arduino UNO microcontrollers	₱2000.00
24V and 5V DC power sources	₱250.00
USB cable	₱50.00
Speaker	₱200.00
Total:	₱3870.00

Table 3: Schedule

Weeks	Progress
Sept 27 - Oct 3	Coding process, device assembly, and moc up making
Oct 4 - Oct 10	
Oct 11 - Oct 17	
Oct 18 - Oct 24	
Oct 25 - Oct 31	
Nov 1 - Nov 7	
Nov 8 - Nov 14	
Nov 15 - Nov 21	
Nov 22 - Nov 28	Experiment and data collection
Nov 29 - Dec 5	
Dec 6 - Dec 12	
Dec 13 - Dec 19	
Dec 20 - Dec 26	
Dec 27 - Jan 2	Finalization (Analysis, and interpretation)
Jan 3 - Jan 9	